2010-09

Team 2: Robust Port Security

Wong, Ka-Yoon

Team 2: Robust Port Security

TEAM 2 MEMBERS

Ka-Yoon Wong
Anderson, Ben LT
Lorenzen, Jesse LT
Macaskill, Jonathan LT
Thompson, Meredith
Naval Postgraduate School, US

Decraene, James
Nanyang Technological University, Singapore

Lobo, Victor
Portuguese Naval Academy, Portugal

Loechel, Alexander
University der Bundeswehr, Germany

Schubert, Johan
Swedish Defence Research Agency, Sweden

INTRODUCTION

Nearly a decade after the highly publicized small boat attacks against the USS Cole (in 2000) and M/V Limburg (in 2002) in Yemen, small vessels continue to pose a security threat to ports worldwide. At ports, small vessels frequently operate in close proximity to important maritime infrastructure, such as bridges and petrochemical plants, and to passenger and military ships. (Department of Homeland Security, Small Vessel Security Strategy, 2008)

An attacker can be easily camouflaged among innocent small vessel traffic and avoid detection by being in the crowd, all the while approaching its desired target undetected and unopposed. When the attacker finally decides to execute the attack, separating from the main traffic to speed toward its target, there is only a narrow time window for an effective defender response.

Two factors confound the defense against such attacks. The first is the lack of warning, which leads to the inability of a defender to anticipate the true target of the attack from among the many possible targets and hence is unable to pre-position any assets to protect the target. The second factor is that the effort to classify the malicious intention of a would-be attacker is non-trivial, since the attacker would look like an innocent vessel from afar. Conceivably, a further difficulty the defender would face is the restriction of maneuver space for an interception attempt in a shipping channel with high traffic, especially if the terrorist boat weaves in and out among the innocent vessels.

The objective of the study is to explore the effects of neutrals on the effectiveness of the defender's deterrence and interdiction operations against a small boat attack in a port environment. The goal of the team was to identify robust employment tactics of port security forces to detect, defend and/or intercept a spectrum of threats and adversary tactics, through the use of MANA and a red-teaming process.

Scenario and Modeling

The Port of Lisbon was chosen for the study scenario. Lisbon is a wealthy and important city, with its busy port contributing significantly to commerce and trade. The city of Lisbon is also a key tourist icon in Portugal, being one of the oldest cities of the world, richly endowed with history dating from the Neolithic era, and is also home to two UNESCO World Heritage Sites – Belém Tower and Jerónimos Monastery (Wikipedia). The city and port present many potential targets for terrorists to strike from the sea and, together with the high volume of traffic in a narrow straits, poses a challenge for the navy and maritime police to defend.

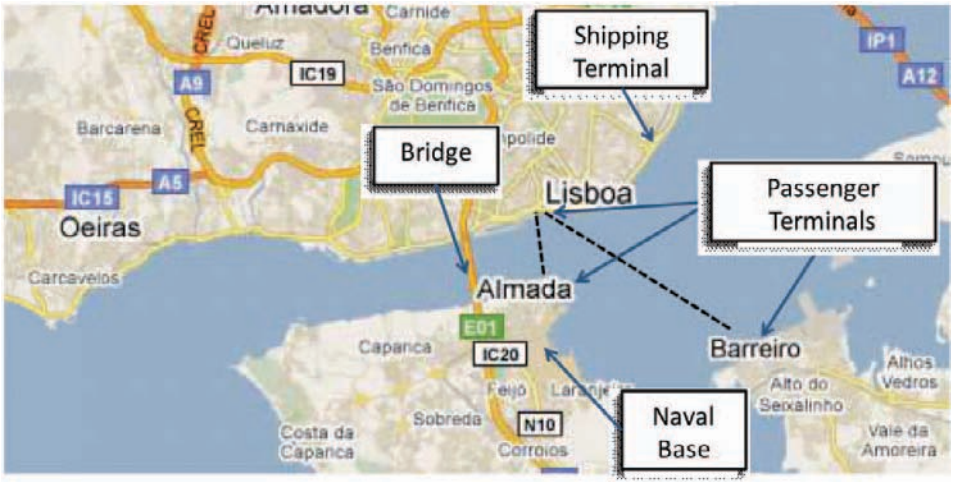

Figure 1: Port of Lisbon

A busy section of the Tagus River at Lisbon, of approximately 10 by 5 km, was modelled (see Figure 1). Initial

runs with the terrain map crashed due to insufficient pixels, but this issue was overcome by increasing the pixel resolution.

Three types of agents are modelled:

- **Neutrals**: Commercial and recreational shipping traffic (neutral vessels) ply the channel in the center of the straits.
- **Attacker**: The attacker is presumed to employ a speedboat in the 20-foot class, such as the Baja Outlaw 20, and is capable of carrying 4 to 6 persons, or a few hundred pounds of explosives, at high speeds. The attacker seeks to be camouflaged among traffic, entering the region from the west, and joining the stream of neutral vessel traffic.
  One intention of the team was to model the attacker's ability to randomly choose a target along the coast to attack. However, due to the complexity of modelling and calibrating the behaviour of the neutral vessels, which consumed most of the time at the workshop, this objective was set aside. Instead, the attacker was given just one target – the naval base on the east of the area of operations considered.
  If the attacker boat is unopposed in its approach to the target, it will follow the shipping traffic until it reaches the shortest path to the target, at which point the attacker will speed up to maximum speed and execute a strike. This modus operandi simulates a high level of surprise that can be accorded to the attacker.
- **Defender**: The defending boats are assumed to be patrol boats equivalent to the SAFE Boat International Defender class boat, widely used by the US Coast Guard. They are tasked to perform random checks on vessels in the channel, and are either deployed in a barrier patrol profile or to sweep the channel (see Figure 2).

Figure 2: Patrol Locations and Attacker's Target

Agent Interactions

Each patrol boat selects a neutral vessel within its sensor range at random, proceeds toward it and stops the vessel for inspection. The inspection takes 5 minutes to complete, after which the vessel will be tagged as a non-threatening vessel and will not be stopped if it later meets other patrol boats.

During an inspection, the patrol boat will be unable to classify any other vessel in its sensor range. After an inspection, the patrol boat will travel for 5 minutes before looking for the next vessel to inspect, to avoid getting fixed in a single location. These two 5 minute gaps potentially allow for an attacker to sneak past the patrol boats.

On the other hand, if the patrol boat stops and inspects an attacker boat, the attacker will be known immediately, and the interception will be counted a success. If the attacker sees the patrol boat, it will speed up and attempt to outrun the defending patrol boat, and head for its target. The patrol boat will give chase and attempt to stop the attacker. However, the attacker has a head-start that leads to an advantage in the chase (since the maximum speeds of both boats are the same).

Experiment Setup

The probability of at least 1 successful attack is used as the Measure of Effectiveness (MOE) in this study. A small experiment was designed to verify the model in the workshop, using the factor and level settings given in Table 1.

Factors	Levels
Number of Neutrals	8 - 20
Number of Blue patrol boats	1 - 3
Number of Red attackers	1 - 3
Speed of Blue patrols	Patrol speed: 10 - 30 kts (Max: 40 kts)
Evasive Speed of Red Attackers	40 kts (Fixed)
Sensor Range	Det: 3000 - 6000 m Class: 200 - 1000 m

Table 1: Factors and Levels

The Nearly Orthogonal Latin Hypercube design of experiments spreadsheet was used to obtain 33 design points (NOLH spreadsheet, downloaded from harvest.nps.edu), and 50 replications of each design point were run.

RESULTS AND ANALYSIS

We anticipated the effects of the factors as follows:

Factor	Proportion of Successful Attacks
More patrols	Reduced
More attackers	Increased
Longer sensor range	Reduced
Speed of patrols	Increased
More neutral shipping	Increased

Table 2: Anticipated Factor Effects on the MOE

The simulation results were analyzed through a partition tree followed by a logistic fit (see Figure 3), yielding two unexpected findings. We found that the speed of patrols had

marginal effect on the proportion of successful attacks, and a surprise finding that more neutrals had resulted in a higher probability of detection.

Scrutiny of the simulation showed that due to the higher volume of traffic, the patrol boats were spending more time in the centre of the channel. Since the route the attacker takes passes through the center of the channel, the chance of a patrol detecting the attacker was higher. We rationalized that this artifact was a model-specific issue.

Conclusion

Within the short span of the workshop, the team managed to assemble and verify a basic model for exploring the defense against small boat attacks in the complex environment of a port. This experiment opens the way for further study by detailing the scenario and providing the building blocks of agent behavior in a MANA model.

REFERENCES

[1] Department of Homeland Security, United States (2008). Small Vessel Security Strategy. Retrieved from www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf

[2] Wikipedia. Lisbon. http://en.wikipedia.org/wiki/Lisbon

[3] Software Downloads, SEED Center for Data Farming, http://harvest.nps.edu/

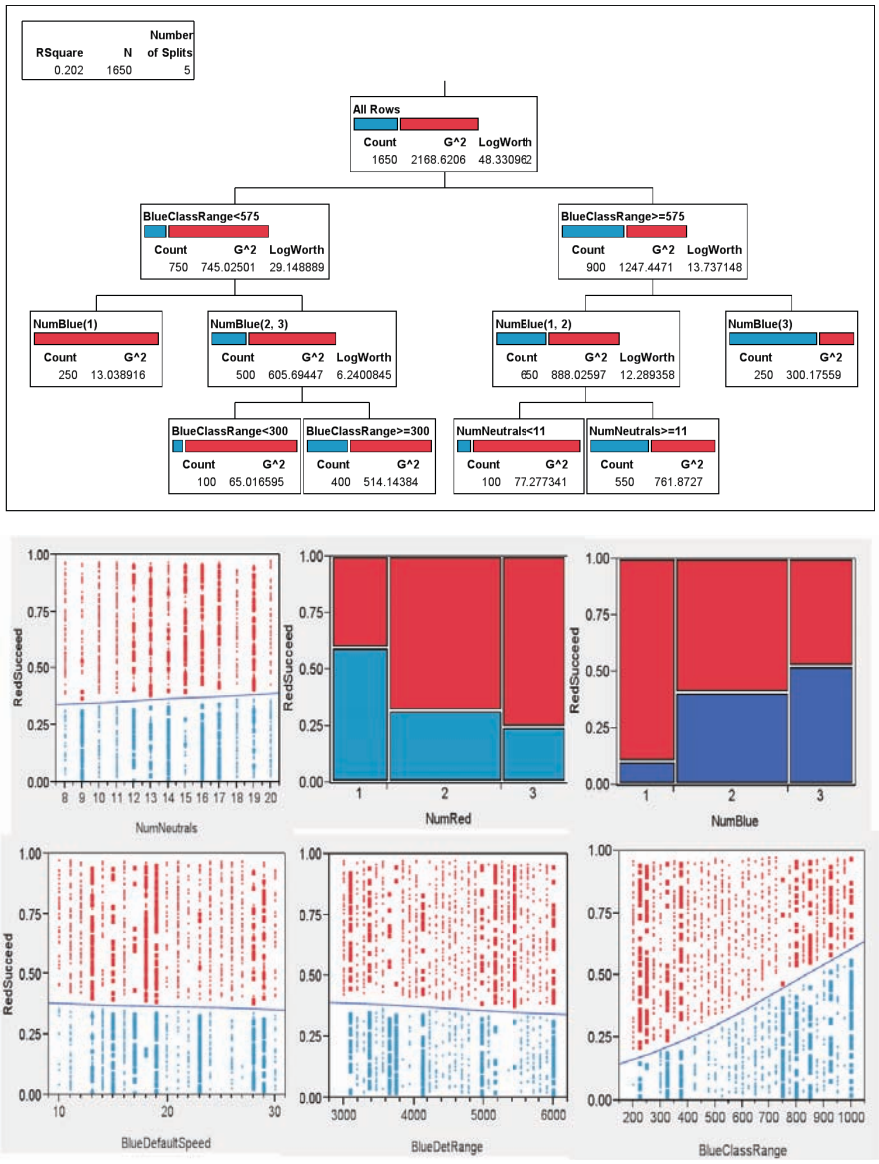

Figure 3: Partition Tree and Logistic FiT